日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ７月１９日

出 願 番 号
Application Number: 平成１１年特許願第２０５３４６号

出 願 人
Applicant (s): インターナショナル・ビジネス・マシーンズ・コーポレイション

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年１１月１９日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆

出証番号 出証特平１１－３０８１５０

【書類名】　特許願

【整理番号】　JA999035

【提出日】　平成11年 7月19日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 15/00

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　堀越　秀人

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　山崎　充弘

【発明者】

【住所又は居所】　神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内

【氏名】　田中　順

【特許出願人】

【識別番号】　390009531

【氏名又は名称】　インターナショナル・ビジネス・マシーンズ・コーポレイション

【代理人】

【識別番号】　100086243

【弁理士】

【氏名又は名称】　坂口　博

【代理人】

【識別番号】　100091568

【弁理士】

【氏名又は名称】　市位　嘉宏

【復代理人】

【識別番号】　100079049

【弁理士】

【氏名又は名称】　中島　淳

【電話番号】　03-3357-5171

【選任した復代理人】

【識別番号】　100084995

【弁理士】

【氏名又は名称】　加藤　和詳

【電話番号】　03-3357-5171

【選任した復代理人】

【識別番号】　100085279

【弁理士】

【氏名又は名称】　西元　勝一

【電話番号】　03-3357-5171

【選任した復代理人】

【識別番号】　100099025

【弁理士】

【氏名又は名称】　福田　浩志

【電話番号】　03-3357-5171

【手数料の表示】

【予納台帳番号】　006839

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9304391

【包括委任状番号】　9304392

【プルーフの要否】　　要

【書類名】　　明細書

【発明の名称】　セキュリティ機能付きコンピュータおよび方法

【特許請求の範囲】

【請求項１】　コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

（ａ）前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第１の記憶手段に記憶し保持するステップと、

（ｂ）前記ステップ（ａ）のあとに前記コンピュータのパワー・オン中または省エネ・モード中に前記コンピュータに前記セキュリティ装置が装着されていることを検出するステップと、

（ｃ）前記ステップ（ｂ）の検出結果を示す装着データを前記コンピュータに装備された第２の記憶手段に記憶し保持するステップと、

（ｄ）前記設定データ及び前記装着データに基づいて前記コンピュータから前記セキュリティ装置が脱着されたことを検出するステップと、

（ｅ）前記ステップ（ｄ）の検出結果に基づいて前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項２】　前記ステップ（ｅ）は所定のパスワードの入力により回避可能であることを特徴とする請求項１に記載の方法。

【請求項３】　コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、

（ａ）前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第１の記憶手段に記憶し保持するステップと、

（ｂ）前記ステップ（ａ）のあとに前記設定データに基づいて前記コンピュータに装備された内蔵基本電源線の連結手段を連結し電力供給線を確保するステップと、

（ｃ）前記コンピュータに前記セキュリティ装置が装着されて前記内蔵基本電

源の電力供給路を形成しているときに前記連結手段の連結を遮断するステップと、

（ｄ）前記ステップ（ｃ）における前記連結の遮断を維持するステップと、

（ｅ）前記連結の遮断により前記コンピュータへのアクセスを禁止するステップと

を有する方法。

【請求項４】　前記ステップ（ｄ）は、前記コンピュータの前記内蔵基本電源の電力供給により維持することを特徴とする請求項３記載の方法。

【請求項５】　セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第１の記憶手段と、

前記コンピュータの主電源が停止しかつ副電源が作動している状態で記憶保持が可能な第２の記憶手段と、

演算処理装置と、

ａ）前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第１の記憶手段に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータのパワー・オン中または省エネ・モード中に前記コンピュータに前記セキュリティ装置が装着されていることを検出するステップと、（ｃ）前記ステップ（ｂ）の検出結果を示す装着データを前記コンピュータに装備された第２の記憶手段に記憶し保持するステップと、（ｄ）前記設定データ及び前記装着データに基づいて前記コンピュータから前記セキュリティ装置が脱着されたことを検出するステップと、（ｅ）前記ステップ（ｄ）の検出結果に基づいて前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第３の記憶手段と

を有するコンピュータ。

【請求項６】　セキュリティ装置の装着ができるコンピュータであって、

前記コンピュータの主電源が停止している状態で記憶保持が可能な第１の記憶手段と、

内蔵基本電源により作動し内蔵基本電源線を連結する連結手段と、

演算処理装置と、

（ａ）前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第１の記憶手段に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記設定データに基づいて前記コンピュータに装備された内蔵基本電源線の連結手段を連結し電力供給線を確保するステップと、（ｃ）前記コンピュータに前記セキュリティ装置が装着されて前記内蔵基本電源の電力供給路を形成しているときに前記連結手段の連結を遮断するステップと、（ｄ）前記ステップ（ｃ）における前記連結の遮断を維持するステップと、（ｅ）前記連結の遮断により前記コンピュータへのアクセスを禁止するステップとを前記コンピュータに実行させるプログラムとを記憶したコンピュータによる読みとりが可能な第２の記憶手段と

を有するコンピュータ。

【請求項７】　前記第１の記憶手段がＲＦＩＤシステムに使用するＲＦＩＤタグであり、前記セキュリティ装置がＲＦアンテナ及び第１接続手段である請求項５または６に記載のコンピュータ。

【請求項８】　前記ＲＦアンテナ及び第１接続手段が前記コンピュータのデバイス・ベイの蓋に装着されている請求項５乃至請求項７のいずれかに記載のコンピュータ。

【請求項９】　前記連結手段がアナログスイッチである請求項６乃至請求項８のいずれかに記載のコンピュータ。

【請求項１０】　前記セキュリティ装置がＲＦアンテナ、第１接続手段及び第２接続手段である請求項９に記載のコンピュータ。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、コンピュータの盗難および不正アクセス等を防止するためにコンピュータ本体に取り外し可能に装着されたセキュリティ機能の一部を担う装置が取り外された場合に、コンピュータへのアクセスを禁止する技術に関する。

【０００２】

【従来の技術】

ノートブック型コンピュータは携帯性に優れている反面、きわめて容易に不正に外部に持ち出される。近年のコンピュータ利用の高度化および多様化に伴い、ユーザは貴重な情報をコンピュータ内部に格納する傾向がますます強まり、コンピュータが盗難に合うとその物理資源の損失に比べて情報資源の漏洩による損失が一層甚大になってきている。

【０００３】

特開平８－５０６９０号公報および特開平１０－１２４７６４号公報は、ＲＦ（ラジオ周波数）トランスポンダ・システムという非接触的な通信技術を用いた電子式物品監視システムを開示する。ＲＦトランスポンダ・システムは、一般的に励振器（Ｅｘｉｃｔｅｒ）／読取器（Ｒｅａｄｅｒ）すなわちＥＲ、およびＲＦＩＤトランスポンダあるいはＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）タグと呼ばれるものを含んでいる。監視区域内の物品にＲＦＩＤタグを取り付け、その領域の出入口にＥＲを設置して常時ＲＦ励振信号を発生させる。出入口にＲＦＩＤタグが取り付けられた物品が接近するとＥＲがこれに励振信号を送信して電力を与えるのでＲＦＩＤタグ自体は特に動作用の電力を必要としない。ＲＦ励振信号を受け取ったＲＦＩＤタグは識別コードその他のデータ信号を発生し、特定の周波数でＥＲに応答信号として送り返す。この応答信号中に含まれる識別コードをＥＲが検出すると必要に応じてアラーム音を発生して物品の盗難を防止する。物品を監視区域内からアラーム音を発生させないで持ち出すには、ＲＦＩＤタグをアラーム信号を送信しない状態にセットするかこれを脱着する必要がある。

【０００４】

特開平５－３５３５４号公報は、ノートブック型コンピュータの盗難防止を図る技術を開示する。ノートブック型コンピュータに、設置傾斜量、設置圧力および設置距離等の設置状態の変化を検出する盗難防止手段と設置状態の変化に応答して警報を発する手段を設ける。これらの手段が機能を発揮する状態にあるときコンピュータは設置状態を常時監視し、コンピュータを許可なく定位置から持ち

運ぼうとした際に警報を発して盗難を防止する。

【０００５】

特開平３－１００８９４号公報は、携帯端末が盗難に合ったときにキー入力を停止して不正なアクセスを禁止する技術を開示する。携帯端末が盗難に合うと、ホストコンピュータから無線で端末に特定の信号を送り、それに応答して端末内部のプログラムが作動してキー入力ができない状態にする。

【０００６】

【発明が解決しようとする課題】

上述したようにＲＦＩＤタグを使用して物品の盗難を防止する技術が知られており、またノートブック型コンピュータが監視区域から不正に持ち出されることを防止する技術およびコンピュータの盗難時にキー入力をロックして情報資源を保護する技術も知られている。しかし、ＲＦＩＤタグをコンピュータに装着して盗難に合ったコンピュータへの不正アクセスを防止する技術は開示されていない。

【０００７】

ところで、盗難防止または記憶情報への不正アクセスを防止するには、コンピュータにＲＦＩＤタグのような装置を装備する必要がある。一方このような装置は、すべてのユーザが必要とするものではなく、一般に企業内で大規模に使用している場合に比べて個人的範囲でのみ使用するユーザにとっては必要性が少ない。セキュリティ機能をすべてのコンピュータに装備して販売することは、必要のないユーザに対して余分な費用を強いることになり好ましくない。したがって、特定のシリーズに含まれる同一タイプのコンピュータにおいて、セキュリティ機能を装備するものとセキュリティ機能を装備しないものとを用意する必要がある。

【０００８】

ところで、特定のシリーズに含まれるコンピュータは、できるだけハードウエアおよびソフトウエアの共通化を図ることが販売コストおよび販売後のサービスの維持という面で好ましい。特定のシリーズのコンピュータをセキュリティ機能を装備するものと装備しないものとに分けて製造および販売することは、一見セ

キュリティ機能を必要としないユーザの費用負担を公平にできるようにみえるが、共通化ができない部分での費用負担が増加し結果としてそのようなユーザにとっても不利になる。ここに、ハードウエアおよびソフトウエアの共通化とユーザによるセキュリティ機能の選択による費用負担の公平性という課題を同時に解決する必要が生じてくる。

【０００９】

これを解決する方法として、あるセキュリティ機能が複数のハードウエアおよびソフトウエアの構成要素からなる場合にその構成要素のある部分までを共通にし、残りの一部を販売店またはユーザが必要に応じて追加できるオプショナル部品にしてセキュリティ機能を完成できるようにする方法がある。しかし、セキュリティ機能の一部を担う装置をユーザまたは販売店で装着するようにすると（このような装置を以後単にセキュリティ装置という。）、その部分が不正に脱着されてセキュリティ機能が毀損されてしまうことが予測される。

【００１０】

したがって本発明の目的は、コンピュータのセキュリティ機能を担う一部の装置、すなわちセキュリティ装置がコンピュータから脱着されたときに、コンピュータへのアクセスを禁止する技術を提供することにある。また、本発明の他の目的は、ユーザまたは販売店がオプショナルに取り付けるセキュリティ装置の好適な取り付け構造を提供することにある。

【００１１】

【課題を解決するための手段】

本発明に係るコンピュータはセキュリティ装置をオプショナルに取り付けることができる構造を備え、セキュリテイ装置を装着することによりセキュリティ機能を具備したコンピュータを構成し、セキュリティ装置を脱着することでセキュリティ機能を具備しないコンピュータを構成する。本発明においてコンピュータへのアクセスを禁止する手順は、コンピュータのパワー・オン、省エネ・モード、特に最小エネルギ・モード等の特定のイベントに関連付けて開始させることができるが、常時ＣＰＵにポーリングにより監視させてもよい。特定のイベントに関連付けて開始させると、ＣＰＵの負担を軽くすることができる。

【００１２】

本発明の第１の態様では、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（ａ）前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第１の記憶手段に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記コンピュータのパワー・オン中または省エネ・モード中に前記コンピュータに前記セキュリティ装置が装着されていることを検出するステップと、（ｃ）前記ステップ（ｂ）の検出結果を示す装着データを前記コンピュータに装備された第２の記憶手段に記憶し保持するステップと、（ｄ）前記設定データ及び前記装着データに基づいて前記コンピュータから前記セキュリティ装置が脱着されたことを検出するステップと、（ｅ）前記ステップ（ｄ）の検出結果に基づいて前記コンピュータへのアクセスを禁止するステップとを備える。

【００１３】

本発明においてセキュリティ装置とは、コンピュータのセキュリティ機能の一部を担うハードウエアであって、オプショナル部品として用意されユーザまたは販売店で脱着可能な程度の装着容易性を備える装置をいう。例えばＲＦＩＤを利用したセキュリティ・システムではＲＦアンテナでもよく、指紋検出を利用したセキュリティ・システムでは指紋入力部であってもよい。さらにセキュリティシステムではジャンパ等の接続部材を含んでいる。第１の記憶手段はコンピュータの主電源が停止した状態で記憶内容を保持できる記憶媒体でＥＥＰＲＯＭまたはハードディスク等を選定できる。さらに２次電池により主電源が停止している場合でも記憶保持ができる電力が供給され続けているＲＡＭであってもよい。また、第２の記憶手段は主電源が停止しかつ副電源（電池や省エネ・モードによる電源）が作動している場合に記憶保持ができ電力が供給され続けているＲＡＭや回路素子等を選定できる。また、コンピュータには電池等の内蔵基本電源が備えられており、この内蔵基本電源ではコンピュータの構成情報等の基本的な構成情報をバックアップするためのＣＭＯＳメモリに電力供給される。この手順はセキュリティ機能を備えるコンピュータおよび備えないコンピュータのいずれに対して

も共通に実行でき、セキュリティ機能を備えるコンピュータについてのみセキュリティ装置が脱着されたときにアクセスが禁止される。

【００１４】

上記第１の態様においては、ステップ（ａ）により、このコンピュータがセキュリティ機能を備えるべく設定した設定データが記憶される。この設定データは、セキュリティ装置の装着前に設定してもよいし、装着後に設定してもよい。このコンピュータがセキュリティ機能を備えたコンピュータであることがシステムにより認識され、コンピュータからセキュリティ装置が脱着された場合は不正行為があったものとして以下の手順によりパスワードを入力しない限りコンピュータへのアクセスが禁止される。ステップ（ｂ）により、このコンピュータがセキュリティ機能を備えるコンピュータであることが確認される。この確認は、セキュリティ装置に導通部位を有させ、この導通部位が存在することを検知することによって可能となる。そして、ステップ（ｃ）によりコンピュータに対するセキュリティ装置の装着または脱着の状態が保持される。保持はメモリのみならずフラグ設定やカウンタ等の計数によっても可能である。次に、ステップ（ｄ）により、セキュリティ装置の脱着が確認され、セキュリティ装置が装着状態から脱着したとき、これは不正行為としてステップ（ｅ）でコンピュータへのアクセスが禁止される。適正にセキュリティ装置を脱着する場合は、パスワードを入れてアクセスを確保することができる。

【００１５】

本発明の第２の態様は、コンピュータに装着されたセキュリティ装置が脱着されたあとに前記コンピュータへのアクセスを禁止する方法であって、（ａ）前記コンピュータに前記セキュリティ装置を装着することを設定した設定データを前記コンピュータに装備された第１の記憶手段に記憶し保持するステップと、（ｂ）前記ステップ（ａ）のあとに前記設定データに基づいて前記コンピュータに装備された内蔵基本電源線の連結手段を連結し電力供給線を確保するステップと、（ｃ）前記コンピュータに前記セキュリティ装置が装着されて前記内蔵基本電源の電力供給路を形成しているときに前記連結手段の連結を遮断するステップと、（ｄ）前記ステップ（ｃ）における前記連結の遮断を維持するステップと、（ｅ

）前記連結の遮断により前記コンピュータへのアクセスを禁止するステップとを備える。

【００１６】

上記第２の態様では、ステップ（ｂ）においてリチウムバッテリ等の連結すなわち内蔵基本電源の電力線を導通させる。この導通は、アナログスイッチ等の連結手段により可能である。これにより、セキュリティ機能を備えていないコンピュータであっても内蔵基本電源が遮断されることがない。ステップ（ｃ）では、一旦セキュリティ装置が装着されてこのコンピュータがセキュリティ機能を備えるコンピュータであることをシステムが認識したのちでセキュリティ装置により内蔵基本電源の電力供給路が形成されているときに連結を遮断する。これは、セキュリティ装置により内蔵基本電源の電力供給路が形成されているため、連結を解除しても内蔵基本電源が遮断されることがないためである。ステップ（ｄ）では、連結の遮断を維持している。この連結の遮断は初期化の困難性が必要があるため、内蔵基本電源の電力供給によりなされることが好ましい。セキュリティ装置が取り外された場合、そのコンピュータに対して不正なアクセスであるときは内蔵基本電源の電力供給路が絶たれ内蔵基本電源から電力供給されていたコンピュータ内部のものが初期化されるので、ステップ（ｅ）によりコンピュータへのアクセスが禁止される。

【００１７】

本発明の第１の態様及び第２の態様で説明した各ステップは、コンピュータ・プログラムによりコンピュータ上で実行させることができる。このようなプログラムは第３の記憶手段として利用できるＥＥＰＲＯＭまたはＦＬＡＳＨ　ＲＯＭといわれる不揮発性のメモリや、ハードディスク、フロッピー・ディスク等に記憶させることができ、コンピュータの動作時にメイン・メモリに読み出して演算処理装置で実行させることができる。

【００１８】

本発明の第３の態様では、第１の記憶手段はコンピュータの主電源が停止している状態で記憶保持できるので、セキュリティ装置の装着についての設定が消去されることはない。また第２の記憶手段は、主電源が停止しかつ副電源が作動し

ている状態で記憶保持が可能である。この副電源は、上記のように電池や省エネ・モードによる電源を選定でき、より広範囲の素子や回路を利用できる。

【００１９】

本発明の第４の態様では、内蔵基本電源により作動する連結手段で内蔵基本電源線を連結する。これにより内蔵基本電源線からの電力供給線を確保できる。コンピュータにセキュリティ装置が装着されて内蔵基本電源の電力供給路を形成しているときには連結手段の連結を遮断する。これはセキュリティ装置による電力供給路が形成され、連結手段の連結が２重の連結になるからである。この連結の遮断は維持され、この状態でセキュリティ装置が脱着されると、内蔵基本電源の電力供給が絶たれるので、内蔵基本電源の電力供給により保持されていた情報例えば設定情報やパスワードが消去され、コンピュータへのアクセスが禁止される。

【００２０】

本発明のセキュリティ装置は、デバイス・ベイの蓋部に組み込むことで、コンピュータの余分なスペースを消費することなくオプショナル部品とすることができる。デバイス・ベイの蓋は、セキュリティ装置を組み込んだ蓋とセキュリティ装置を組み込んでいない単なる蓋の二つをオプショナル部品としていずれか一つを選択できるようにし、ユーザまたは販売店でコンピュータに装着できる。このセキュリティ部品には、ＲＦアンテナやジャンパ等の接続部材を含んでいる。

【００２１】

【発明の実施の形態】

［コンピュータ・システムの概要］

図１には、本発明を実施するのに適した典型的なノート型パーソナル・コンピュータ１０のハードウェア構成をサブシステム毎に模式的に示している。ＣＰＵ１１は、ＯＳの制御下で、各種プログラムを実行するようになっている。ＣＰＵ１１は、システム・バス１３を経由して、一般にメモリ／ＰＣＩ制御チップ１５と呼ばれるブリッジ回路（ホストーＰＣＩブリッジ）に接続されている。本実施例のメモリ／ＰＣＩ制御チップ１５は、メイン・メモリ１７へのアクセス動作を制御するためのメモリ・コントローラ機能や、システム・バス１３とＰＣＩバス

１９間のデータ転送速度の差を吸収するためのデータ・バッファなどを含んだ構成となっている。

【００２２】

メイン・メモリ１７は、ＣＰＵ１１の実行プログラムの読み込み領域として、あるいは実行プログラムの処理データを書き込む作業領域として利用される、書き込み可能メモリである。ここで言う実行プログラムには、Ｗｉｎｄｏｗｓ９８などのＯＳ、周辺機器類をハードウェア操作するための各種デバイス・ドライバ、特定業務に向けられたアプリケーション・プログラムや、ＦＬＡＳＨ　ＲＯＭ４９に格納されたＢＩＯＳが含まれる。ビデオ・サブシステム２１は、ビデオに関連する機能を実現するためのサブシステムであり、ＣＰＵ１１からの描画命令を実際に処理し、処理した描画情報をビデオ・メモリ（ＶＲＡＭ）に一旦書き込むとともに、ＶＲＡＭから描画情報を読み出して液晶ディスプレイ（図示せず。）に描画データとして出力するビデオ・コントローラを含む。

【００２３】

カードバス・コントローラ２３は、ＰＣＩバス１９のバス・シグナルをＰＣＩカード・スロット２５のインタフェース・コネクタ（カードバス）に直結させるための専用コントローラである。ＰＣＩバス１９とＩ／Ｏバス３９とは、多機能ＰＣＩデバイス２７によって相互接続されている。本実施例の多機能ＰＣＩデバイス２７は、ＰＣＩバス１９とＩ／Ｏバス３９とのブリッジ機能、ＤＭＡコントローラ機能、プログラマブル割り込みコントローラ（ＰＩＣ）機能、及びプログラマブル・インターバル・タイマ（ＰＩＴ）機能、　ＩＤＥ（Ｉｎｔｅｇｒａｔｅｄ　Ｄｒｉｖｅ　Ｅｌｅｃｔｒｏｎｉｃｓ）インタフェース機能、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）機能、ＳＭＢ（Ｓｙｓｔｅｍ　Ｍａｎａｇｅｍｅｎｔ　Ｂｕｓ）インタフェース機能を備えており、たとえば、インテル社より提供されているＰＩＩＸ４というデバイスを選択することができる。ＩＤＥインタフェースには、ＩＤＥハードディスク・ドライブ（ＨＤＤ）３１が接続される他、ＩＤＥ　ＣＤ－ＲＯＭドライブ３２が接続される。また、ＩＤＥ　ＣＤ－ＲＯＭ３２ドライブの代わりに、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｉｄｅｏ　Ｄｉｓｃ又はＤｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｃ）ドライブのよ

うな他のタイプのＩＤＥ装置が接続されていても良い。ＨＤＤ３１やＣＤ－ＲＯＭドライブ３２のような外部記憶装置は、例えばシステム１０本体内の「メディア・ベイ」又は「デバイス・ベイ」と呼ばれる収容場所に格納される。これら標準装備された外部記憶装置は、ＦＤＤやバッテリ・パックのような他の機器類と交換可能かつ排他的に取り付けられる場合もある。

【００２４】

多機能ＰＣＩデバイス２７にはＲＦＩＤタグとしての機能を発揮するＲＦＩＤチップ３３が接続される。ＲＦＩＤチップ３３にはＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８が接続される。ＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８は、ＨＤＤ３１をコンピュータ１０に収納するためのデバイス・ベイの蓋部に組み込まれている。セキュリティ機能を必要としないユーザは、ＲＦアンテナ３７が組み込まれていないデバイス・ベイの蓋を選択することができる。すなわち、セキュリティ装置の一部としてのＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８はオプショナル部品であり、ユーザ自らがまたは販売店において、ＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８が付加されたアンテナ付き蓋またはアンテナ無し蓋のいずれか一方を装着することができる。ＲＦＩＤチップ３３は、リーダ／ライタが発信したＲＦ励振信号をＲＦアンテナ３７で受信して処理し、コンピュータの不正な持ち出しや不正なアクセスを禁止するセキュリティ機能を備えている。

【００２５】

また、本実施例では、ＲＦＩＤチップ３３には、セキュリティ機能をより強固なものとするためにリチウムバッテリー３４に接続されている。このリチウムバッテリー３４は、周知のように、システムメモリ領域に現在のシステム構成情報を保持するメモリ（所謂ＣＭＯＳメモリ）５０を不揮発性とするために電力を供給したり内蔵時計をバックアップするために電力を供給したりするため、通常交換が困難なバッテリ電源である。これらの要素はコンピュータ１０のセキュリティ機能の一部を分担しており、後に動作の概要を説明する

Ｉ／Ｏバス３９としては、例えばＩＳＡバスがあり、Ｓｕｐｅｒ　Ｉ／Ｏコントローラ４１、電源コントローラ４５、ＦＬＡＳＨ　ＲＯＭ４９、メモリ（所謂

ＣＭＯＳメモリ）５０等が接続される。Ｓｕｐｅｒ　Ｉ／Ｏコントローラ４１は、フロッピー・ディスク・ドライブ（ＦＤＤ）の駆動、パラレル・ポートを介したパラレル・データの入出力（ＰＩＯ）、シリアル・ポートを介したシリアル・データの入出力（ＳＩＯ）を制御するための周辺コントローラで、Ｉ／Ｏポート４３が接続される。電源コントローラ４５は主としてシステム内のパワー・マネジメントやサーマル・マネジメントを行うシングル・チップ・マイコンで、日立製作所から提供されるＨ８／３００チップを選定することができる。電源コントローラ４５は、ＭＰＵ、ＲＡＭ、ＲＯＭおよびタイマ等を備え、ＲＯＭにはパワー・マネジメントやサーマル・マネジメントを実行するのに必要なプログラムおよび参照テーブルを格納している。電源コントローラ４５には、パワー・サプライ・コントローラ４７が接続されている。パワー・サプライ・コントローラ４７にはバッテリィを充電するための充電器およびコンピュータ１０で使用する５Ｖ、３．３Ｖ等の一定電圧を生成するためのＤＣ／ＤＣコンバータが含まれ、電源コントローラ４５のもとで直接的に電力制御を行う。

【００２６】

ＦＬＡＳＨ　ＲＯＭ４９は、キーボードやフロッピー・ディスク・ドライブ（ＦＤＤ）などの各ハードウェアの入出力操作を制御するためのコード群（ＢＩＯＳ：Ｂａｓｉｃ　Ｉｎｐｕｔ／Ｏｕｔｐｕｔ　ｓｙｓｔｅｍ）や、電源投入時の自己診断テスト・プログラム（ＰＯＳＴ：Ｐｏｗｅｒ　Ｏｎ　Ｓｅｌｆ　Ｔｅｓｔ）などのファームウェアを恒久的に格納するための書き換え可能な不揮発性メモリである。メモリ（所謂ＣＭＯＳメモリ）５０は、システムメモリ領域に現在のシステム構成情報を保持するためにリチウムバッテリー３４から電力が供給されるメモリである。なお、コンピュータ・システム１０を構成するためには、図１に示した以外にも多くの電気回路等が必要である。但し、これらは当業者には周知であり、また、本発明の要旨を構成するものではないので、本明細書中では省略している。

［ＲＦＩＤを利用したセキュリティ機能］

ＲＦＩＤとは一般にＲＦ（Ｒａｄｉｏ　ｆｒｅｑｕｅｎｃｙ）すなわ無線を使ってＩＤ（ｉｄｅｎｔｉｆｉｅｒ）をＥＥＰＲＯＭに読み書きする機能であるとい

うことができる。ＲＦＩＤは単に無線を使った情報交換にとどまらず、一方にリーダ／ライタを配置し他方にＲＦＩＤタグを配置した場合に両者間で情報交換するためにＲＦＩＤタグが電源を必要としないところに最大の特徴がある。リーダ／ライタはＲＦＩＤタグにＲＦ励振信号を送り、ＲＦＩＤタグを励振して電力を発生させてデータを書き込みまたその電力を利用してＲＦＩＤタグがデータをリーダ／ライタに送り返す。このようなＲＦＩＤによるデータの読み書き機能を利用して、電源が停止したコンピュータとリーダ・ライタとの間で多くの情報を交換することができコンピュータの在庫管理等に利用できる。

【００２７】

ＲＦＩＤの他の利用形態としてコンピュータのセキュリティ機能に関するものがある。図２は、ＲＦＩＤタグとしてのＲＦＩＤチップ３３の内部構成を概略的に記載したものである。このようなＲＦＩＤチップとしては、ＡＴＭＥＬ社から提供されるＡＴ２４ＲＦ０８という型式のＥＥＰＲＯＭ（Ａｓｓｅｔ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ＥＥＰＲＯＭ）がある。ＲＦＩＤチップ３３に含まれるＥＥＰＲＯＭ５５は、記憶領域が８Ｋビットの一般エリア５７と２５６ビットの特殊エリア５９に分割されている。一般エリア５７には、ＲＦアンテナ３７で受信したＲＦ励振信号のデータがアナログ・インタフェース５３を経由して書き込まれ、また書き込まれているデータはインタフェース５３およびＲＦアンテナ３７を経由して発信される。またＥＥＰＲＯＭ５５とコンピュータ１０はシリアル・インタフェース６１およびＳＭＢ３５を通じて通信し、コンピュータから一般エリア５７および特殊エリア５９への書き込みおよび読み出しができる。

【００２８】

ここで、特殊エリア５９には１つの記憶領域が設けられている。それは、ＲＦアンテナの装着検出の設定を示すＲｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットである。このＲｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットは、予め用意されたセットアップユーティリティでオプションパーツとしてＲＦアンテナを装着するときに設定するものであり、適切なパスワードを保有するユーザが設定することにより、「１」がセットされる。なお、初期状態すなわち未装着のときは「０」すなわちリセットされている。一般エリア５７には、２つの記憶領

域が設けられている。その一つは、ＲＦアンテナの装着状況の履歴を示すＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットで、コンピュータ１０へＲＦアンテナが装着されたことが検出されると「1」にセットされる。もう一つは、Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットで、一旦装着されたＲＦアンテナ３７が脱着されたことが検出されると「1」にセットされる。Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビット、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよびアンテナ　Ｅｒｒｏｒビットは適切なパスワードを保有するユーザがＳＭＢ３５およびシリアル・インタフェース６１を経由してコンピュータ・システムからＥＥＰＲＯＭ５５にアクセスしない限りリセットできない。

【００２９】

特殊エリア５９には、ＲＦアンテナ３７のコンピュータ１０に対する着脱状態を検出するためのＤＥ／ＤＣビット領域、ＲＦアンテナ３７が監視区域のゲード近くに設置されたリーダ／ライタからＲＦ励振信号を受信したときにセットするＴａｍｐｅｒビット領域、一般エリア５７へのリード、ライトをロックするＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビット領域、およびコンピュータの電源がオフになるまでＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットの変更をロックするＳｔｉｃｋｙビット等が含まれる。Ａｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットは２ビットで構成され、「００または０１」のときは一般エリアへの一切のアクセスが禁止され、「１０」のときは読み出しだけが許可され、「１１」のときは書き込みおよび読み出しが許可される。

【００３０】

ＤＥ／ＤＣビット領域は、ＤＥビット（Ｄｅｔｅｃｔ　Ｅｎａｂｌｅ　ｂｉｔ）とＤＣビット（Ｄｅｔｅｃｔ　Ｃｏｉｌ　ｂｉｔ）からなる。ＲＦＩＤチップ３３は、シリアル・インタフェース６１を通じてＤＥビットが「1」にセットされるとＲＦアンテナ３７の着脱状態をチェックし、ＲＦアンテナ３７が装着されているときは「1」を、脱着されているときは「0」をＤＣビットに書き込むようになっている。コンピュータの電源が入っている場合は電源部５１がアナログ・インタフェース５３を駆動するが、電源がない場合はＲＦアンテナ３７を通じて受信したＲＦ励振信号がアナログ・インタフェース５３を駆動し、電源がない

状態でもリーダ／ライタと通信できる。

【００３１】

また、本実施例では、ＲＦＩＤチップ３３は、デジタルインタフェース６２を含んでいる。デジタルインタフェース６２は、ＮＡＮＤ素子６３、フリップフロップ回路６５、アナログスイッチ６７を含んでおり、特殊エリア５９に書きこまれているＲｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットの状態（「１」または「０」）がハイレベル信号またはローレベル信号として、アナログスイッチ６７の制御側及びＮＡＮＤ素子６３の一方の入力側に出力される構成になっている。ＮＡＮＤ素子６３の他方の入力側はフリップフロップ回路６５を介して端子７１に接続されている。本実施例では、フリップフロップ回路６５として所謂Ｄフリップフロップを用いており、入力側（Ｄ端子）に端子７１が接続され、不論理出力側（／Ｑ端子）にＮＡＮＤ素子６３の他方の入力側が接続されている。このフリップフロップ回路６５の入力側（Ｄ端子）と端子７１の間は抵抗６９を介して電源に接続されている。端子７１と一対である端子７３は接地されており、第１短絡素子３６の接続で端子７１と端子７３とが短絡する。これにより、フリップフロップ回路６５の入力側（Ｄ端子）は、第１短絡素子３６が接続されることでローレベルとなり、離間することによりハイレベルとなる。なお、図示は省略したが、フリップフロップ回路６５にはシステムクロック及びリセット信号が入力されるように接続されている。ＮＡＮＤ素子６３の出力側は、第１短絡素子３６の接続状態（接続又は離間）を出力するために、電源コントローラ４５に接続されている。このＮＡＮＤ素子６３の出力信号は、後述するキーボード等の入力操作を禁止するためのＩＮＴＲ信号として機能する。なお、ＮＡＮＤ素子６３、上記フリップフロップ回路６５、及び抵抗６９へ電力を供給する電源は、電源コントローラ４５の基の電力制御に連動し、電源投入後はもとより、所謂スタンバイ時、サスペンド時のように電力の消費を抑制する省電力モード時にも電力が供給されるものとする。

【００３２】

アナログスイッチ６７の一方の端子はリチウムバッテリー３４のプラス側に直接接続され端子７７に接続されている。端子７７と一対である端子７５は、リチ

ウムバッテリー３４に直接接続されるべき、上記システム構成情報を保持するメモリ（所謂ＣＭＯＳメモリ）５０の電源に接続されると共に、アナログスイッチ６７の他方の端子が接続される。Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットの状態が「１」であるときは、アナログインタフェース５３を介してハイレベル信号がアナログスイッチ６７に供給されて、アナログスイッチ６７は非導通となる。これにより、ＣＭＯＳメモリにはアナログスイッチ６７を介してのリチウムバッテリー３４の電力供給がされることはない。一方、Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットの状態が「０」であるときは、ローレベル信号がアナログスイッチ６７に供給されて、アナログスイッチ６７は導通する。これにより、ＣＭＯＳメモリとリチウムバッテリー３４とはアナログスイッチ６７を介して導通電されることになる。従って、Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットの状態が「１」であるときは、第２短絡素子３８の接続で端子７５と端子７７とが短絡することにより、ＣＭＯＳメモリにはリチウムバッテリー３４の電力供給がなされ、第２短絡素子３８の離間によりＣＭＯＳメモリへのリチウムバッテリー３４の電力供給が遮断される。なお、アナログスイッチ６７にはリチウムバッテリー３４から直接電源供給されており、システムの電源状態に関わらずスイッチ状態を維持できるものとする。また、本実施例では、ハード構成を用いて説明するが、本発明はこれに限定されるものではなく、ソフトウェア構成でもよい。

［本発明の実施例を適用するセキュリティ機能の概要］

次に本発明の実施例を適用するコンピュータのセキュリティ機能の概要を説明する。電源がオフになっているコンピュータが監視区域のゲートに近づくと、リーダ／ライタが発信するＲＦ励振信号がＲＦアンテナ３７に送られ、ＥＥＰＲＯＭ５５の特殊エリア５９にＴａｍｐｅｒビットがセットされる。つぎにコンピュータの電源を投入すると、ＦＬＡＳＨ　ＲＯＭ４９に格納されているＢＩＯＳがメイン・メモリ１７に書き込まれ、ＣＰＵ１１はＰＯＳＴおよびシステムの初期化を実行する。ＰＯＳＴがＴａｍｐｅｒビットを検出するとパスワードの入力をユーザに要求すると共にその時点でＰＯＳＴの実行を停止し、パスワードの入力がない限りコンピュータへアクセスすることはできなくなる。

【００３３】

前述のようにＲＦアンテナ３７はユーザまたは販売店が装着できるようにしているため、不正にコンピュータを外に持ち出そうとする者がＲＦアンテナ３７を外してからゲートを通過し、Ｔａｍｐｅｒビットがセットされるのを回避しようとする可能性がある。本発明の実施例では、ＲＦアンテナ３７はオプションとして取り付けるが、その他のハードウエアはＲＦアンテナ３７を装着する場合と脱着する場合とで共通である。また、ＲＦアンテナ３７を装着する場合とＲＦアンテナを脱着する場合のいずれにおいても同一のソフトウエア（ＢＩＯＳ）を採用できる。以下において、ＲＦアンテナ３７が脱着された場合にコンピュータへのアクセスを禁止するための手順の実施例を説明する。

【００３４】

［基本手順を示す例］

まず、本発明の実施例を説明するのに先だって、電源がオフの状態でＲＦアンテナが不正に外された後、そのまま電源がオンにされた場合にコンピュータへのアクセスを禁止するための基本手順を説明する。

【００３５】

図３は電源がオンの状態でＲＦアンテナが外された後、そのまま電源がオンにされた場合にコンピュータへのアクセスを禁止する基本手順を含むフローチャートである。コンピュータ１０にＲＦアンテナが実際に装着されてセキュリティ機能が有効になるか否かは、この時点でシステムにとって不明である。コンピュータ１０のＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよびビットは、工場から出荷する時点では共に「０」にセットされている。ブロック１０１でコンピュータ１０の電源をオンにすると、ＢＩＯＳがＦＬＡＳＨＲＯＭ４９からメイン・メモリ１７に読み出され、ＣＰＵ１１がＰＯＳＴプログラムを読みとって以下の手順を実行する。ＲＦＩＤチップ３３は、電源投入時点では常にＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットが「１１」にＳｔｉｃｋｙビットが「１」にセットされ、一般エリア５７へのＢＩＯＳによるアクセスが許可される。ブロック１０３でＰＯＳＴは現実にＲＦアンテナ３７がコンピュータに装着されているか否かを確認するために特殊エリア５９のＤＥビットを「１」

にセットする。これに応じてＲＦＩＤチップ３３はＲＦアンテナ３７の装着状態をチェックし、装着されていればＤＣビットに「１」を脱着されていれば「０」を書き込む。

【００３６】

ＰＯＳＴはＤＥビットを「１」にセットしてから約２００マイクロ秒経過した後ＤＣビットを読みとり、さらにＤＥビットを「０」にセットする。ＤＣビットが「１」にセットされて現在ＲＦアンテナ３７が装着されていることが確認されたならばブロック１０５に移行して一般エリア５７のＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットを「１」にセットする。この時点で、コンピュータ１０がセキュリティ機能を具備するコンピュータであることがシステムによって認識されたことになり、以後Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットは、パスワードを有するユーザが書き換えない限り電源がオフになってもこの情報を維持し続ける。ＤＣビットが「０」でＲＦアンテナが脱着されていることが確認されたならば、プロック１０７に移行して一般エリア５７のＡｎｔｅｎｎａ　Ｅｒｒｏｒビットを確認する。Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットをこの時点で確認することは、後にブロック１０９で詳細に説明するが、前日のＰＯＳＴを実行する以前に一旦装着されたＲＦアンテナが脱着されたことがあったか否かを確認することに相当する。

【００３７】

ブロック１０７でＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」のときは、前回のＰＯＳＴを実行する以前にＲＦアンテナ３７が一旦装着され、さらに前日のＰＯＳＴを実行する段階でＲＦアンテナ３７が脱着されていた場合であり、ＲＦアンテナの不正な脱着があったものとしてこれを処理するブロック１１９に移行する。以後Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットは、パスワードを有するユーザが書き換えない限り電源がオフになってもこの情報を維持し続ける。ブロック１０７でＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「０」のときは、すくなくとも前日のＰＯＳＴの実行時点まではＲＦアンテナの不正な脱着がなかったものと判断し、ブロック１１１に移行する。

【００３８】

ブロック１１１では、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットを確認する。す

なわち、今回のＰＯＳＴを実行する時点までにＲＦアンテナ３７がコンピュータ１０に装着されたことがあるか否かを確認する。Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットへのデータは、ブロック１０５により今回のＰＯＳＴ実行時に、または前日以前のＰＯＳＴ時に書き込まれる。ブロック１１１でＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットが「０」のときは、現在までＲＦアンテナが装着されたことがない場合であってコンピュータ１０はセキュリティ機能を有しないコンピュータであることを意味しており、ブロック１１５に移行する。ブロック１１１でＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットが「１」のときは、今回のＰＯＳＴを実行する時点までにＲＦアンテナが装着されたことがあり、かつ前回のＰＯＳＴを実行する時点までの間に一旦装着されたＲＦアンテナが脱着されたことがＰＯＳＴで検出されていない場合（Ａｎｔｅｎｎａ　Ｅｒｒｏｒビット＝０）であり、ブロック１１３に移行する。

【００３９】

ブロック１１３ではＤＣビットを再度確認し、今回のＰＯＳＴ実行時点でＲＦアンテナ３７が装着されているか脱着されているかを判断する。ＤＣビットが「１」すなわち現実にＲＦアンテナ３７がコンピュータ１０に装着されていれば、セキュリティ装置の脱着はなかったものとしてブロック１１５に移行する。ＤＣビットが「０」のときは、今回のＰＯＳＴを実行する以前にＲＦアンテナが装着されていたが（ブロック１１１）今回のＰＯＳＴを実行する段階では脱着されており（ブロック１１３）、さらに前回のＰＯＳＴを実行する以前に一旦装着されたＲＦアンテナが前回以前のＰＯＳＴを実行する段階で脱着されたことが検出されていない（ブロック１０７）場合であり、ブロック１０９に移行して処理される。言い換えると、これは前回のＰＯＳＴを実行してから今回のＰＯＳＴを実行するまでの間にＲＦアンテナが脱着された場合を今回のＰＯＳＴで処理する手順である。前回のＰＯＳＴを実行する時点においてそれまでに一旦装着されたＲＦアンテナ３７が脱着されていると、前回のＰＯＳＴを実行する時点でＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」にセットされ、今日のＰＯＳＴを実行するとブロック１０７からブロック１１９に移行して処理されるからである。

【００４０】

ブロツク１１５は、ブロック１１１から移行する手順で示されるセキュリティ機能を有しないコンピュータと、ブロック１１３から移行する手順で示されるセキュリティ機能を有しかつＲＦアンテナ３７が一旦装着された後に脱着されたことがないコンピュータとを処理する。この場合は、セキュリティ装置の脱着はないので、Ａｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットを「１０」にセットし、以後一般エリアのＡｎｔｅｎｎａ　ＨｉｓｔｏｒｙビットおよびアンテナＥｒｒｏｒビットへの書き込みを禁止する。さらにＳｔｉｃｋｙビットを「０」にセットして、コンピュータの電源が切られるまでＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットの変更ができないようにする。これは、ＯＳ経由でＡｃｃｅｓｓ　Ｐｒｏｔｅｃｔｉｏｎビットが「１１」に変更され、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットまたは Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットの内容が書き換えられるのを防止するためである。この結果Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットおよび Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットの書き換えは、電源がオンになったブロック１０１からブロック１１５までの間だけ可能になり、実際はこの間にＰＯＳＴだけがビットの書き換えをすることになる。続いてブロック１１７に移行し、ＢＩＯＳはブートストラップを実行し、ＯＳおよびアプリケーション・プログラムをメイン・メモリに読み出しコンピュータの構成を行う。

【００４１】

ブロック１０９ではＡｎｔｅｎｎａ　Ｅｒｒｏｒビットを「１」に書き換える。Ａｎｔｅｎｎａ　Ｅｒｒｏｒビットは ＰＯＳＴを実行する毎にブロック１０７ないしブロック１１３が判断され、その結果に応じて「１」に書き換えられる。ブロック１０９は、前日のＰＯＳＴを終了した時点ではＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」に書き換えられていなかったが（ブロック１０７）、今回のＰＯＳＴを実行した時点で過去においてＲＦアンテナ３７が装着されたことがある（ブロック１１１）にも係わらず現在それが脱着されている（ブロック１１３）場合を処理する。

【００４２】

続いてブロック１０９からブロック１１９に移行する。さらにブロック１０７で判断したＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」である場合もブロック１

１９に移行する。ブロック１１９では今回のＰＯＳＴを実行する間にブロック１０９によりＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」にセットされた場合および前回のＰＯＳＴを終了するまでの間にＡｎｔｅｎｎａ　Ｅｒｒｏｒビットが「１」であったことに応答してコンピュータ１０のディスプレイにＰＯＳＴエラーの表示をする。

【００４３】

次にブロック１２１でディスプレイにユーザにパスワードを要求するメッセージを表示し、ＢＩＯＳがブロック１２３で正しいパスワードの入力を認識すると、ブロック１２７でＡｎｔｅｎｎａ　ＨｉｓｔｏｒｙビットおよびＡｎｔｅｎｎａ　Ｅｒｒｏｒビットを「０」に書き換える。続いてブロック１２９でＰＯＳＴを再スタートする。再スタートしたＰＯＳＴでは、ＰＯＳＴエラーの表示がでることはなくブロック１０１からブロック１１７までの手順をクリアしてブートストラップが実行される。

【００４４】

ＢＩＯＳがブロック１２３で正しいパスワードを認識しないとその時点でＰＯＳＴは停止し、以後コンピュータへのアクセスはできなくなる。それ以降正しいパスワードを入力できる場合は、再度ブロック１０１の電源オンからスタートして、ブロック１２１で正しいパスワードを入力してからブロック１２９を経由して再度ブートストラップを実行する。

【００４５】

ところで、上記図３のフローチャートで説明した手順では、電源がオンの状態でＲＦアンテナが不正に外されてコンピュータが外部に持ち出されても、一旦電源をオフにしてＰＯＳＴを実行する段階にならないとコンピュータへのアクセスを禁止することはできない。電源オンの状態でＲＦアンテナが外されてしまうことに対処するためには、図４に示すフローチャートにより達成できる。電源が投入され、図３で説明した手順でＰＯＳＴが実行されてブートストラップが開始されると、デバイス・ドライバによってブロック１５１から手順が開始される。ブロック１５３ではＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットが確認される。今回のＰＯＳＴを実行する時にＲＦアンテナが装着されていれば図３のブロック１０５

でＡｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットは「１」にセットされている。ブロック１５３では、Ａｎｔｅｎｎａ　Ｈｉｓｔｏｒｙビットを確認し、ビットが「０」でＲＦアンテナが装着されていなければブロック１５７へ移行し本手順は終了する。

【００４６】

ブロック１５３で確認したビットが「１」で今回のＰＯＳＴを実行した時点でＲＦアンテナが装着されていれば、ブロック１５５に移行する。ブロック１５５でポーリングにより定期的にＤＣビットの状態を確認する。このポーリングは実際には他のプログラムの実行を妨げないように、タイマー・インターラプトなどによって行われることが好ましい。ＲＦアンテナ３７が脱着されない限りＣＰＵはＲＦアンテナの装着状態を定期的に監視する。ＲＦアンテナ３７が脱着されるとブロック１５９に移行しコンピュータの電源が強制的にオフにされるので、ユーザが再度電源をオンにすると図３に示したＰＯＳＴが再スタートさせられる。図３の手順ではブロック１０３、１０７、１１１、１１３、１０９、１１９、１２１のルートに従って処理され、パスワードが要求される。すなわちコンピュータの電源オンの状態において、一旦装着されたＲＦアンテナ３７が脱着されると、ＣＰＵ１１のポーリングのタイミングでコンピュータの電源がオフにされるので、次回の電源をオンにしたときＰＯＳＴが実行され、パスワードを入力できないユーザはそれ以上コンピュータにアクセスできないことになる。

【００４７】

［本発明の手順を示す第１の実施例］

上記基本手順では、電源がオンの状態でＲＦアンテナが不正に外されたときについて、コンピュータへのアクセスを禁止する場合を説明した。本実施例では、スタンバイやサスペンドといわれるような各種省エネ・モード状態でＲＦアンテナが外されてしまうことに対処するためのものである。本発明の手順を示す第１の実施例としてのフローチャートを図５に示す。

【００４８】

図５は本発明の手順を示す第１の実施例としてのフローチャートである。コンピュータ１０の電源をオンにすると、ＢＩＯＳがＦＬＡＳＨ　ＲＯＭ４９からメ

イン・メモリ１７に読み出され、ＣＰＵ１１がＰＯＳＴプログラムを読みとって以下の手順を実行する。まず、ブロック８１で予め用意されたセットアップユーティリティによりオプションパーツのセキュリティ機能を有効にする設定（Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビット＝１）がなされているか否かを判断する。セキュリティ機能無効の設定の場合には、コンピュータへのアクセスを禁止する必要がないため、ブロック８１で否定され、本手順を終了する。なお、図５に示す手順は、定期的に実行されるように実行させることができる。

【００４９】

コンピュータ１０にＲＦアンテナが実際に装着されても、セキュリティ機能を有効にするまでは、機能しない。そこで、適切なパスワードを保有するユーザは、コンピュータ１０にＲＦアンテナが実際に装着されてセキュリティ機能を有効にするために、ＲＦアンテナの装着開始を設定するにあたり、予め用意されたセットアップユーティリティでオプションパーツを設定する。これにより、Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットが「１」に設定される。この場合、ブロック８１で肯定され、これにより、ＲＦＩＤチップ３３は、ハイレベル信号をアナログスイッチ６７の制御側及びＮＡＮＤ素子６３の一方の入力側に出力する。

【００５０】

このとき、図２に示すように、第１短絡素子３６の接続で端子７１と端子７３とが短絡している場合、フリップフロップ回路６５の入力側（Ｄ端子）はローレベルで出力側はハイレベルである。従って、ＮＡＮＤ６３には共にハイレベル信号が入力され、出力であるＩＮＴＲ信号はローレベルである。一方、第１短絡素子３６が離間されると、フリップフロップ回路６５の出力側は１クロック送れてローレベルになる。従って、ＮＡＮＤ６３の出力であるＩＮＴＲ信号はハイレベルになる。すなわち、ＩＮＴＲ信号がハイレベルになる場合には、第１短絡素子３６が離間つまりＲＦアンテナ３７が脱着されたことになる。そこで、ブロック８５でＰＯＳＴはＩＮＴＲ信号（ハイレベル信号）が出力されたか否かを確認し、ＩＮＴＲ信号がハイレベル信号であるとき、第１短絡素子３６が脱着されているとして、ブロック８７に移行してキーボードをロックし、入力不能とすること

によりコンピュータを停止させる。これにより、ＰＯＳＴは停止し、以後コンピュータへのアクセスはできなくなる。一方、ＩＮＴＲ信号がローレベル信号であるとき、第１短絡素子３６が装着されているとして、本手順を終了する。なお、上記図３で説明したブロック１０３へ進み、上述のようにして、電源オン時の手順を実行（ブーストラップ等が開始されたり継続中の処理が再開）してもよい。

【００５１】

このように、電源コントローラ４５の電力制御に連動し、電源投入後はもとより、所謂スタンバイ時、サスペンド時のように電力の消費を抑制する省電力モード時にも電力が供給されている場合に、第１短絡素子３６が脱着されたすなわちＲＦアンテナ３７が脱着された場合には、入力不能とすることによりコンピュータを停止させるので、ＲＦアンテナ３７が脱着された場合にコンピュータへのアクセスを禁止することができる。

【００５２】

［本発明の手順を示す第２の実施例］

上記図５のフローチャートで説明した手順では、電源がサスペンド等の省エネモードの状態でＲＦアンテナが外されたときについて、コンピュータへのアクセスを禁止する場合を説明した。本実施例では、機械的に電源オフ状態にした場合やハイパーネーションといわれるような基本構成部分のみの電源状態でＲＦアンテナが外されてしまうことに対処するためのものである。すなわち、図５のフローチャートで説明した手順では、電源が機械的に遮断または基本構成部分のみの最低電源状態でＲＦアンテナが外されてコンピュータが外部に持ち出し、再度ＲＦアンテナを装着されると、コンピュータへのアクセスを禁止できない。本実施例は、これに対処するためのものである。本発明の手順を示す第２の実施例としてのフローチャートを図６に示す。

【００５３】

本発明の手順を示す第２の実施例としてのフローチャートを図６に示す。コンピュータ１０の電源をオンにすると、ＢＩＯＳがＦＬＡＳＨ　ＲＯＭ４９からメイン・メモリ１７に読み出され、ＣＰＵ１１がＰＯＳＴプログラムを読みとって以下の手順を実行する。まず、ブロック８９で予め用意されたセットアップユー

ティリティによりオプションパーツのセキュリティ機能を有効にする設定がなされているか否かを判断する。セキュリティ機能無効の設定の場合には、コンピュータへのアクセスを禁止する必要がないため、ブロック８９で否定され、本手順を終了する。なお、上記図３で説明したブロック１０３へ進み、上述のようにして、電源オン時の手順を実行（ブーストラップ等が開始されたり継続中の処理が再開）してもよい。

【００５４】

上記説明したように、適切なパスワードを保有するユーザが、コンピュータ１０にＲＦアンテナが実際に装着されてセキュリティ機能を有効にするために、Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットが「１」に設定されると、ブロック８９で肯定され、これにより、ＲＦＩＤチップ３３は、アナログインタフェース５３を介してハイレベル信号をアナログスイッチ６７の制御側に出力する。これにより、ブロック９５でアナログスイッチ６７が作動され、端子７５と端子７７の間の導通が切断される。

【００５５】

Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットの状態が「１」であるときは、第２短絡素子３８の接続で端子７５と端子７７とが短絡することにより、ＣＭＯＳメモリにはリチウムバッテリー３４の電力供給がなされ、第２短絡素子３８の離間によりＣＭＯＳメモリへのリチウムバッテリー３４の電力供給が遮断される。すなわち、Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ　Ｅｎａｂｌｅビットの状態が「１」のままで、第２短絡素子３８が離間つまりＲＦアンテナ３７が脱着されたときには、リチウムバッテリー３４により供給されていた所謂ＣＭＯＳメモリへの電力が遮断される。このため、ＣＭＯＳエラーが発生する。ＣＭＯＳエラーが発生すると、次回の電源オン時に、上記ブロック１１９へ進み（図３に結合子２で示した）、ユーザにパスワードを要求する。このように、正しいパスワードの入力により、ＲＦアンテナ３７が脱着された場合にコンピュータへのアクセスを禁止することができる。

【００５６】

一方、ＣＭＯＳエラーが非発生の場合には、第２短絡素子３８が正しく装着さ

れているものとして、上記図３の手順を実行し、電源がオフの状態でＲＦアンテナが外されてそのまま電源がオンされた場合にコンピュータへのアクセスを禁止する手順を進める。すなわち、図３のブロック１０３から実行する。

【００５７】

このように、本実施例では、電源がオフ状態や最小電力の省エネモードで稼動中のコンピュータで、ＲＦアンテナ３７が脱着された場合であっても、アナログスイッチでリチウムバッテリからのＣＭＯＳへの電源供給を遮断できる。このため、着脱したＲＦアンテナを再度取り付けて、ユーザが再度電源をオンにしてＰＯＳＴが再スタートさせられた場合であっても、一旦装着されたＲＦアンテナ３７が脱着されると、ＣＭＯＳメモリへの電源がオフにされるので、次回の電源をオンにしたときにはＰＯＳＴが実行され、パスワードを入力できないユーザはそれ以上コンピュータにアクセスできないことになる。

【００５８】

図７に本発明を実行するコンピュータ１０の外形の一例を示す。コンピュータ１０は図１で説明した構成要素を収納する本体２０１、液晶ディスプレイ２０３、本体上部に配置したキーボード２０７、ＣＤ－ＲＯＭドライブ３２、およびＨＤＤ３１を収納するデバイス・ベイの蓋２０９を含む。コンピュータ１０はデバイス・ベイの蓋２０９を除いて、本実施例との関連で特別な外形的特徴を備えるものではない。

【００５９】

図８に本発明で使用するＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８の装着方法の実施例を示す。ＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８はデバイス・ベイの蓋２０９に収納される。デバイス・ベイにＨＤＤ３１が着脱可能な状態で装着した後に蓋２０９を本体２０１に対してはめ込み構造で取り付ける。ＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８を使用しない場合、すなわちセキュリティ機能を必要としないコンピュータでは、ＲＦアンテナ３７を取り付けないで蓋２０９だけを本体２０１に装着できる。また、蓋２０９とは異なりＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８を収納できない構造の蓋を用意してもよい。このようなＲＦアンテナ３

７、第１短絡素子３６及び第２短絡素子３８の取り付け構造を蓋２０９に採用することにより、ユーザまたは販売店でＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８の取り付けが可能になり、ユーザはセキュリティ機能の必要性に応じてＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８付きの蓋２０９またはＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８なしの蓋２０９のいずれかを選択できる。蓋２０９の内側には、アンテナ３７用コイルが収納され、そのリード部２１１は蓋２０９の端子部２１３にはめ込まれると共に、ＲＦＩＤチップ３３に電気的に接続される。また、蓋２０９の端子部２１５には、第１のジャンパ端子として機能するリード部の第１短絡端子３６がはめ込まれ、端子部２１７には、第２のジャンパ端子として機能するリード部の第２短絡端子３８がはめ込まれる。

【００６０】

このような方法でＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８を取り付ける場所としては、ＨＤＤ用のデバイス・ベイの蓋部にとどまらずＣＤ－ＲＯＭドライブ、ＤＶＤドライブ、ＦＤＤ、バッテリィ等の外部装置のデバイス・ベイの蓋や、これらを択一的に収納できるマルチ・ベイの蓋を利用できる。ＲＦアンテナ３７、第１短絡素子３６及び第２短絡素子３８の本体２０１に対する取り付け構造は、コンピュータの使用場所において不正行為者が短時間に脱着できるものではなく、かつ販売店またはユーザがある程度の時間を費やして着脱できる程度に強固なものであることが好ましい。たとえば、はめ込み構造に加えてスクリューで締め付ける構造や、そのスクリューに特殊な工具を要するものを採用することができる。

【００６１】

本発明の実施例はＲＦＩＤを利用したセキュリティ装置の脱着が行われたときにコンピュータへのアクセスを禁止する例で説明したが、本発明の適用範囲はＲＦＩＤに限定されるものではなく、たとえば指紋によりコンピュータへのアクセス資格を確認するような他の種類のセキュリティ装置にも適用できる。

【００６２】

以上、本発明を特定の実施例に基づいて説明したが、本発明は、本発明の思想

を考慮して当業者が容易に考えることができるさらに多くの実施例を含むものである。

【００６３】

【発明の効果】

本発明により、セキュリティ装置が脱着されたときにアクセスができなくなるコンピュータを提供することができた。また本発明により、装着および脱着が可能で余分なスペースを必要としないセキュリティ装置の取り付け構造を備えたコンピュータを提供することができた。

【図面の簡単な説明】

【図１】

本発明を実施するコンピュータの概略ブロック図の一例である。

【図２】

本発明め実施例で使用するＲＦＩＤチップの概略ブロック図である。

【図３】

本発明の手順を示す第１の実施例のフローチャートである。

【図４】

基本手順を補足する手順示す例のフローチャートである。

【図５】

本発明の手順を示す第１の実施例のフローチャートである。

【図６】

本発明の基本手順を示す例のフローチャートである。

【図７】

本発明を実施するコンピュータの外形図の一例である。

【図８】

本発明の実施例で使用するＲＦアンテナの取り付け方法の一例を示す図である。

【符号の説明】

３３　　ＲＦＩＤチップ

３４　　リチウムバッテリー

３６　短絡素子

３７　アンテナ

３８　短絡素子

５５　ＥＥＰＲＯＭ

６１　シリアルインタフェース

６２　デジタルインタフェース

６３　ＮＡＮＤ素子

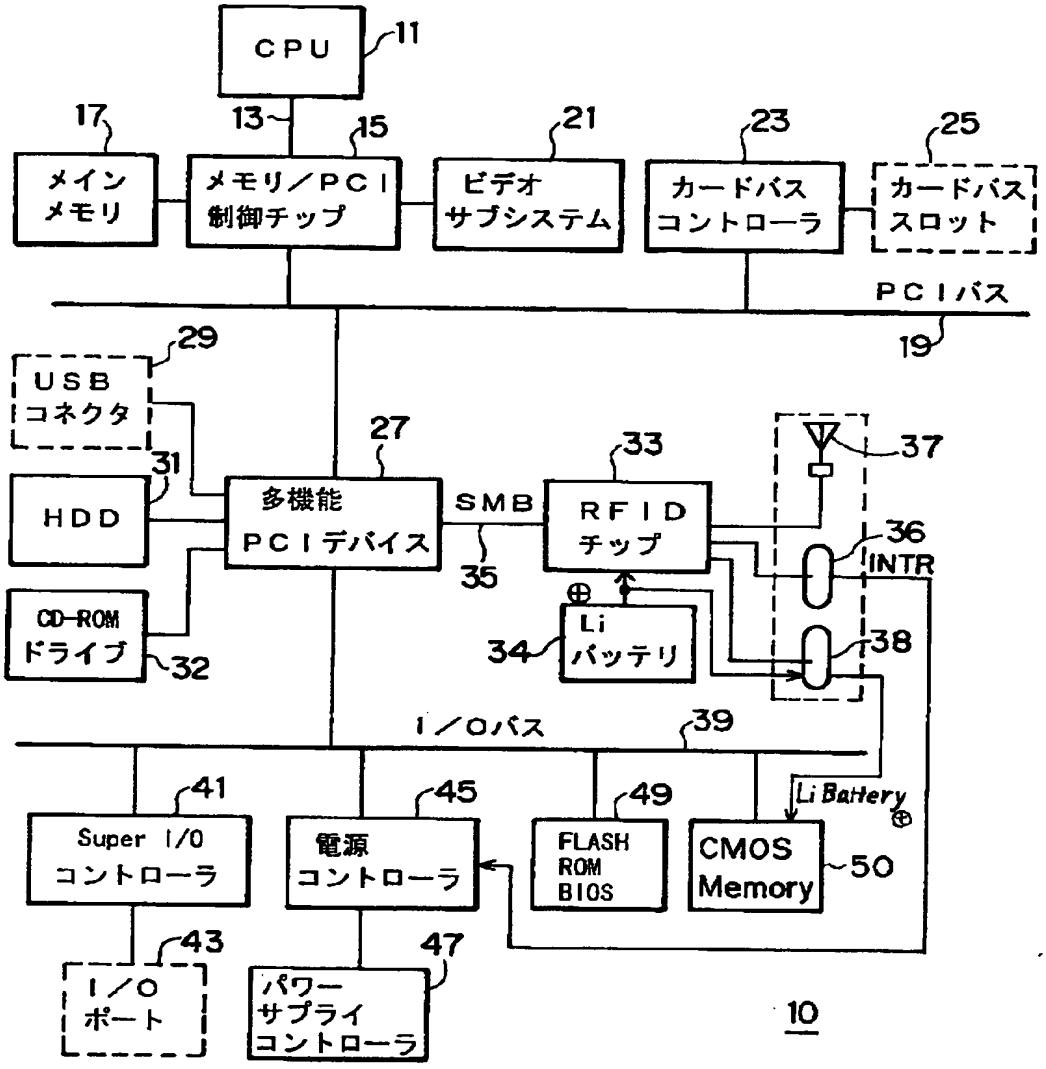
６５　フリップフロップ回路

６７　アナログスイッチ

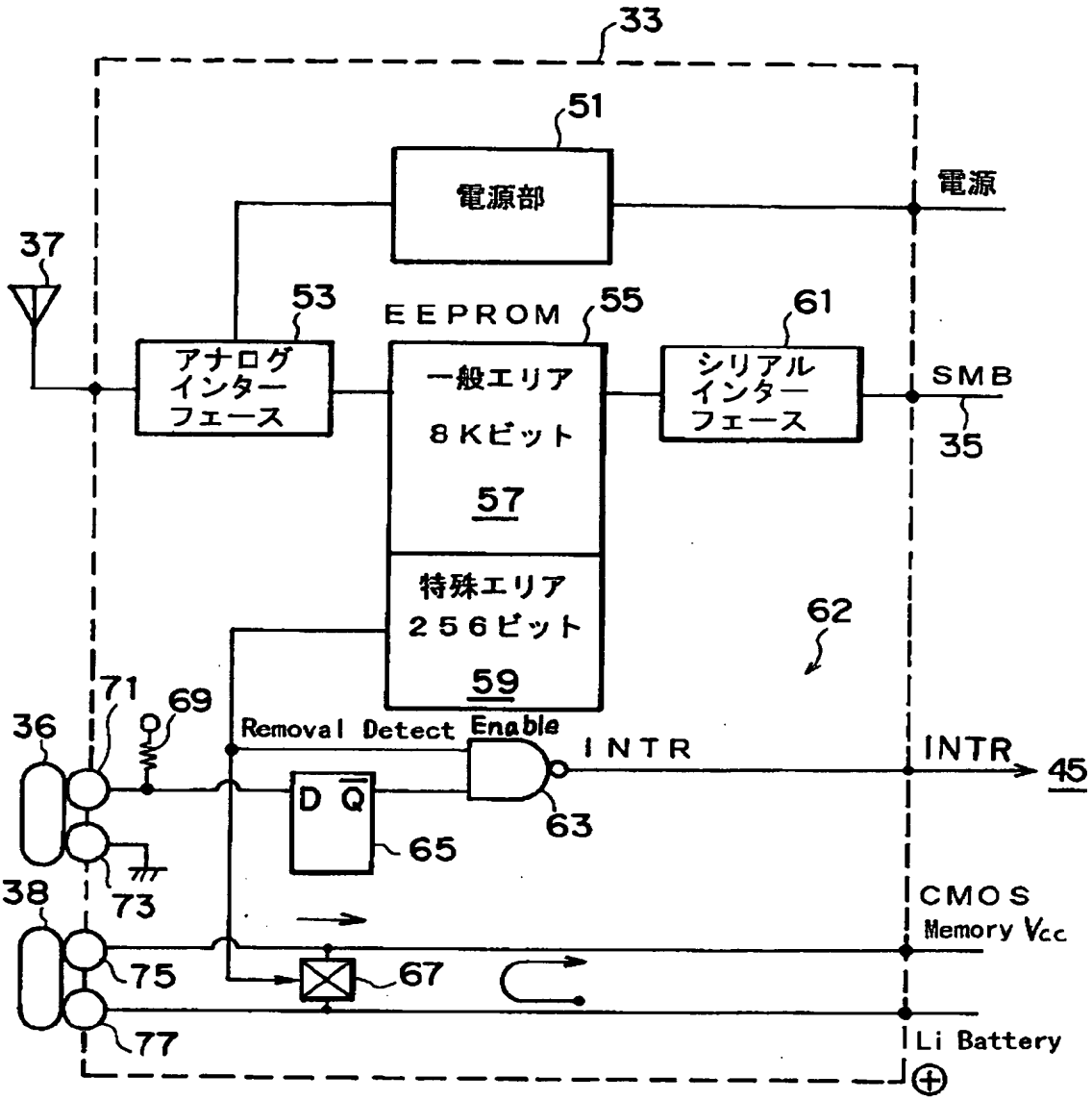
６９　抵抗

【書類名】　　図面

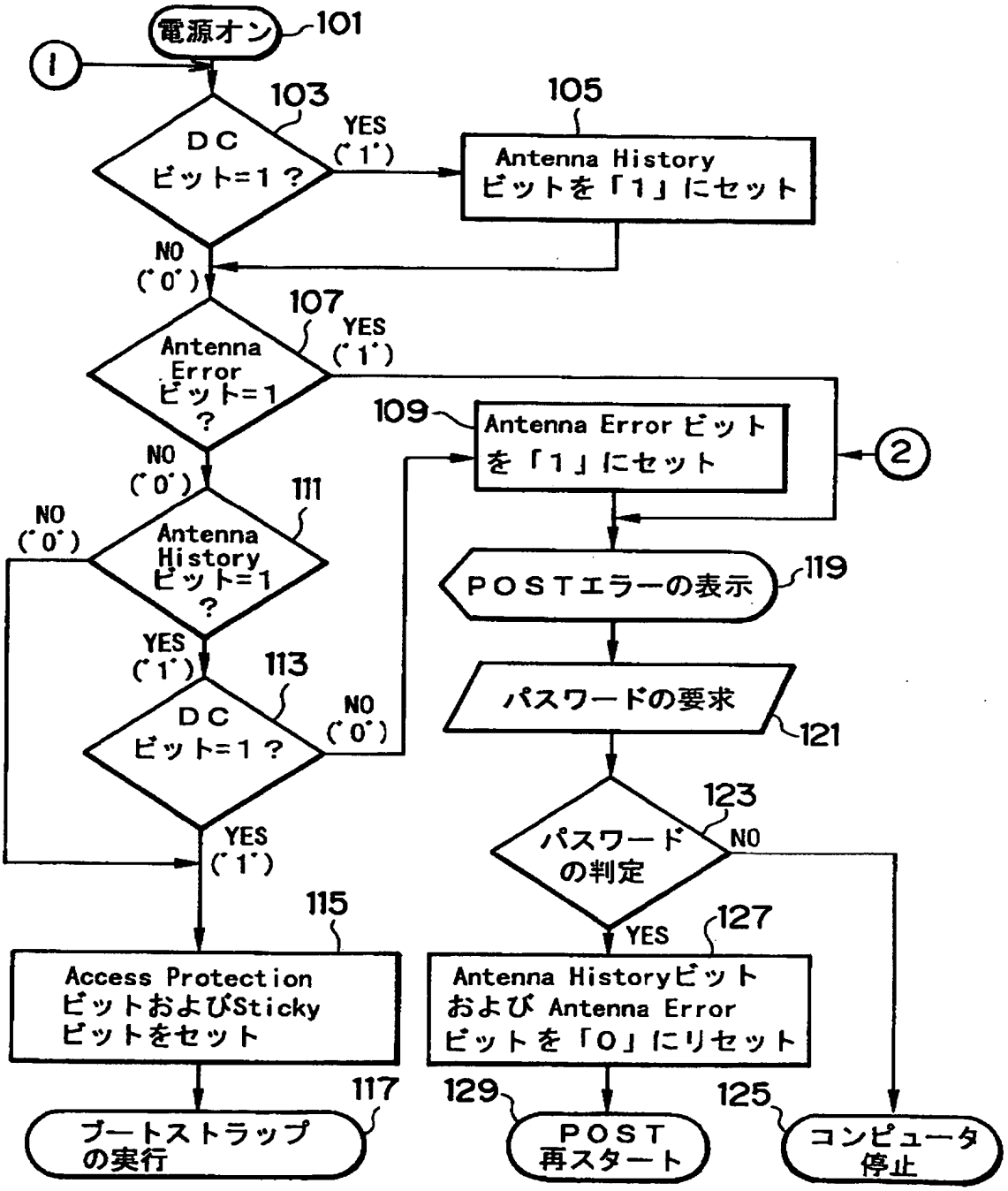
【図１】


CPU
11
17
13
15
21
23
25
メイン
メモリ
メモリ／PCI
制御チップ
ビデオ
サブシステム
カードバス
コントローラ
カードバス
スロット
PCIバス
19
29
USB
コネクタ
27
33
37
31
HDD
多機能
PCIデバイス
SMB
RFID
チップ
36
INTR
35
CD-ROM
ドライブ
32
34
Li
バッテリ
38
I／Oバス
39
41
45
49
Li Battery
Super I/O
コントローラ
電源
コントローラ
FLASH
ROM
BIOS
CMOS
Memory
50
43
47
I／O
ポート
パワー
サプライ
コントローラ
10

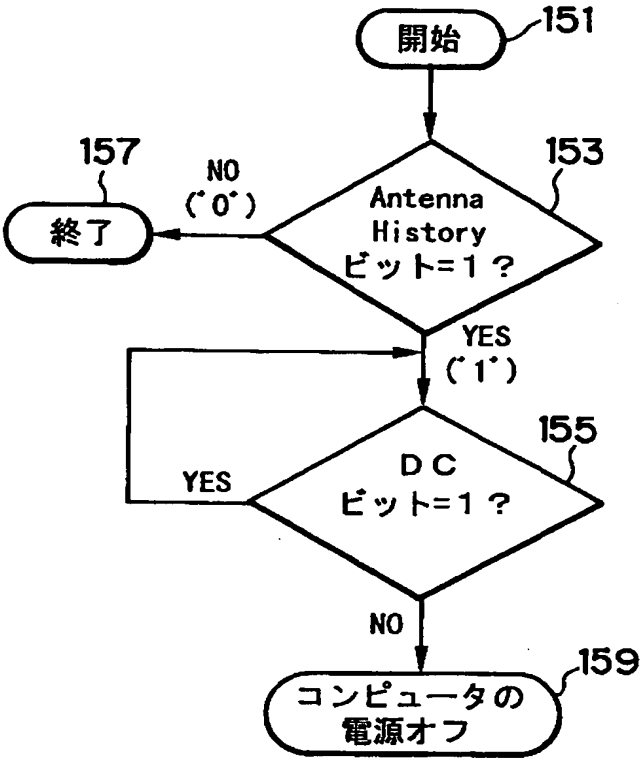
【図２】


33
51
電源部
電源
37
53
EEPROM
55
61
アナログ
インター
フェース
一般エリア
８Kビット
57
シリアル
インター
フェース
SMB
35
特殊エリア
２５６ビット
59
62
71
69
36
Removal Detect Enable
INTR
INTR
45
D Q
65
63
73
38
CMOS
Memory Vcc
75
67
77
Li Battery
⊕

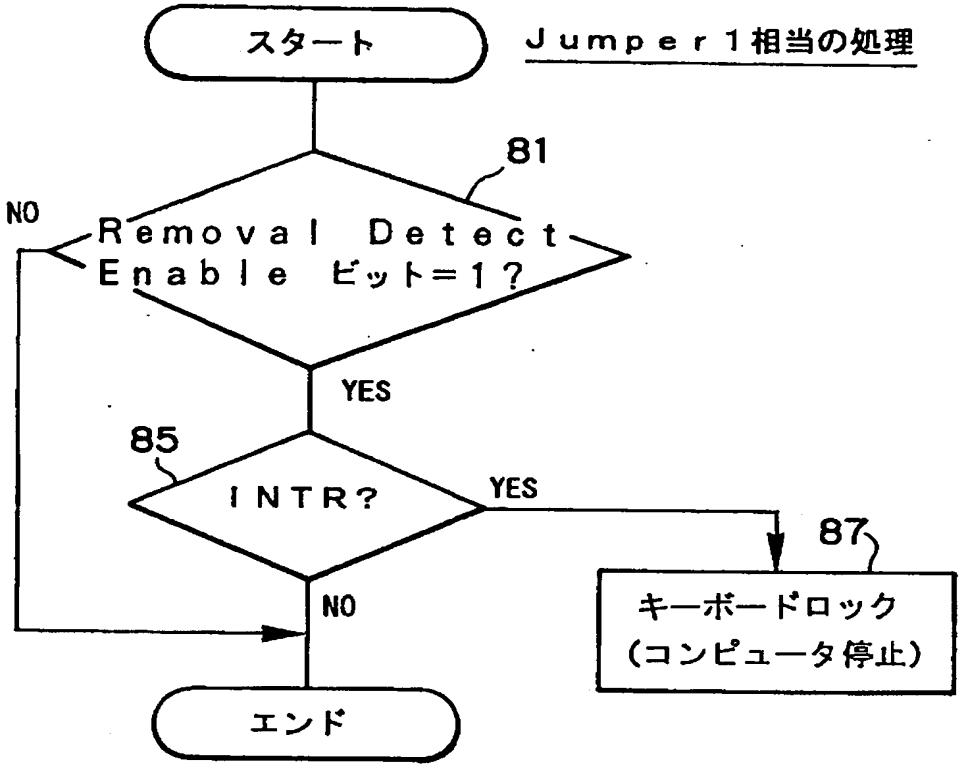
【図３】


電源オン
101
①
103
DC
ビット=1？
YES
('1')
105
Antenna History
ビットを「1」にセット
NO
('0')
107
Antenna
Error
ビット=1
？
YES
('1')
109
Antenna Error ビット
を「1」にセット
②
NO
('0')
111
Antenna
History
ビット=1
？
NO
('0')
YES
('1')
113
DC
ビット=1？
NO
('0')
YES
('1')
115
Access Protection
ビットおよびSticky
ビットをセット
117
ブートストラップ
の実行
POSTエラーの表示
119
パスワードの要求
121
123
パスワード
の判定
NO
YES
127
Antenna Historyビット
および Antenna Error
ビットを「0」にリセット
129
POST
再スタート
125
コンピュータ
停止

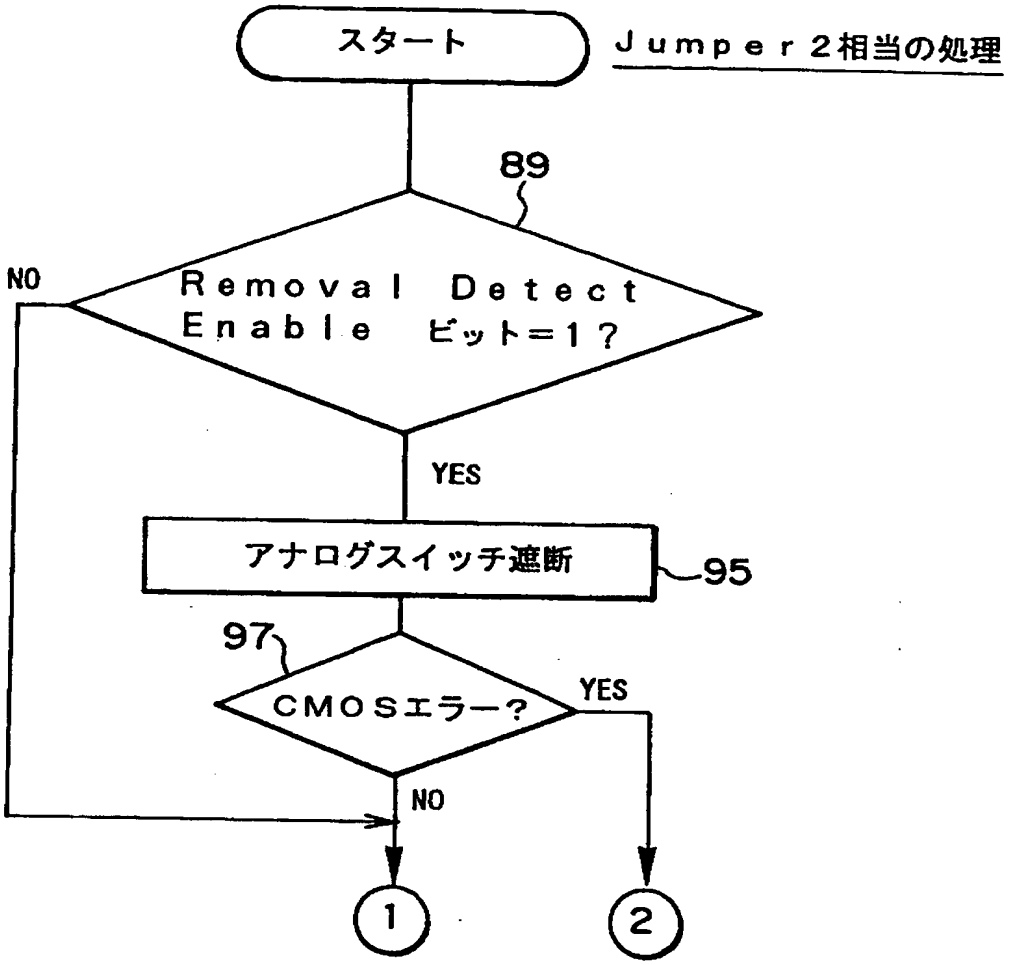
【図４】


開始
151
Antenna History ビット=１？
153
NO ('0')
157
終了
YES ('1')
DC ビット=１？
155
YES
NO
コンピュータの電源オフ
159

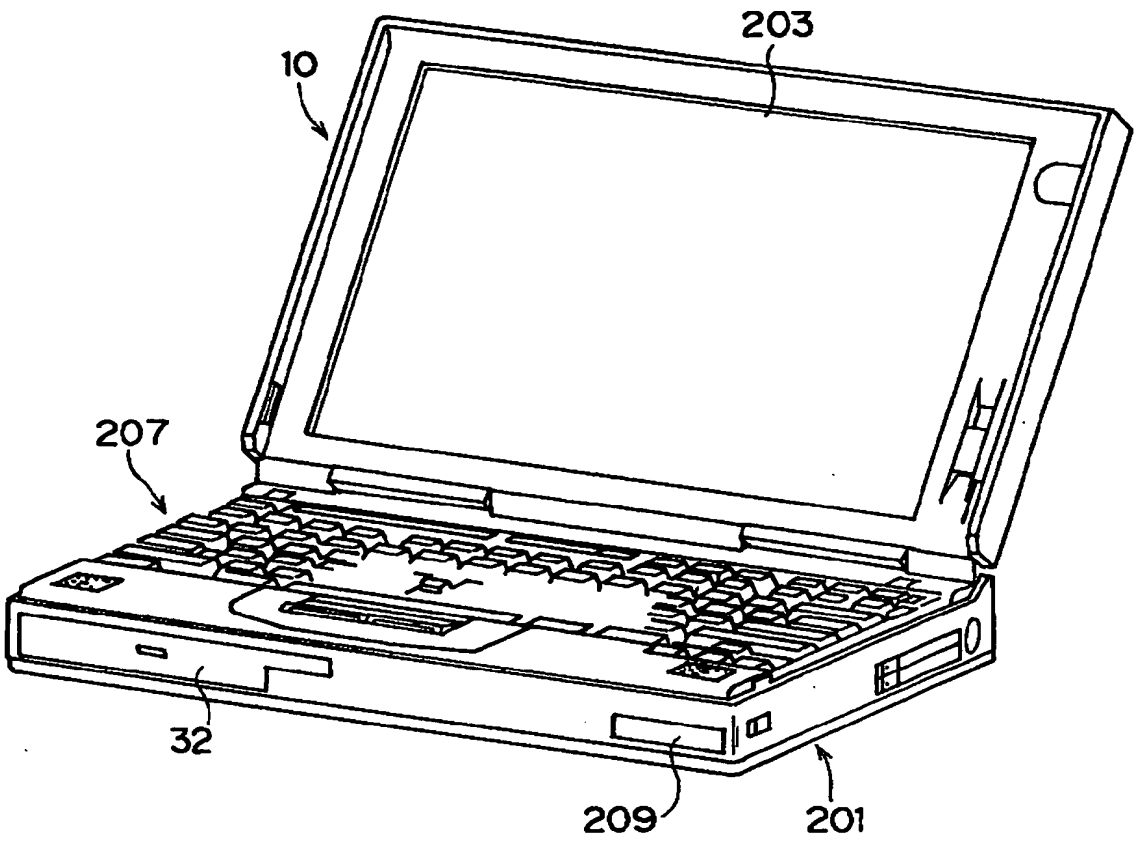
【図５】


スタート
Ｊｕｍｐｅｒ１相当の処理
81
NO
Ｒｅｍｏｖａｌ Ｄｅｔｅｃｔ
Ｅｎａｂｌｅ ビット＝１？
YES
85
ＩＮＴＲ？
YES
87
キーボードロック
（コンピュータ停止）
NO
エンド

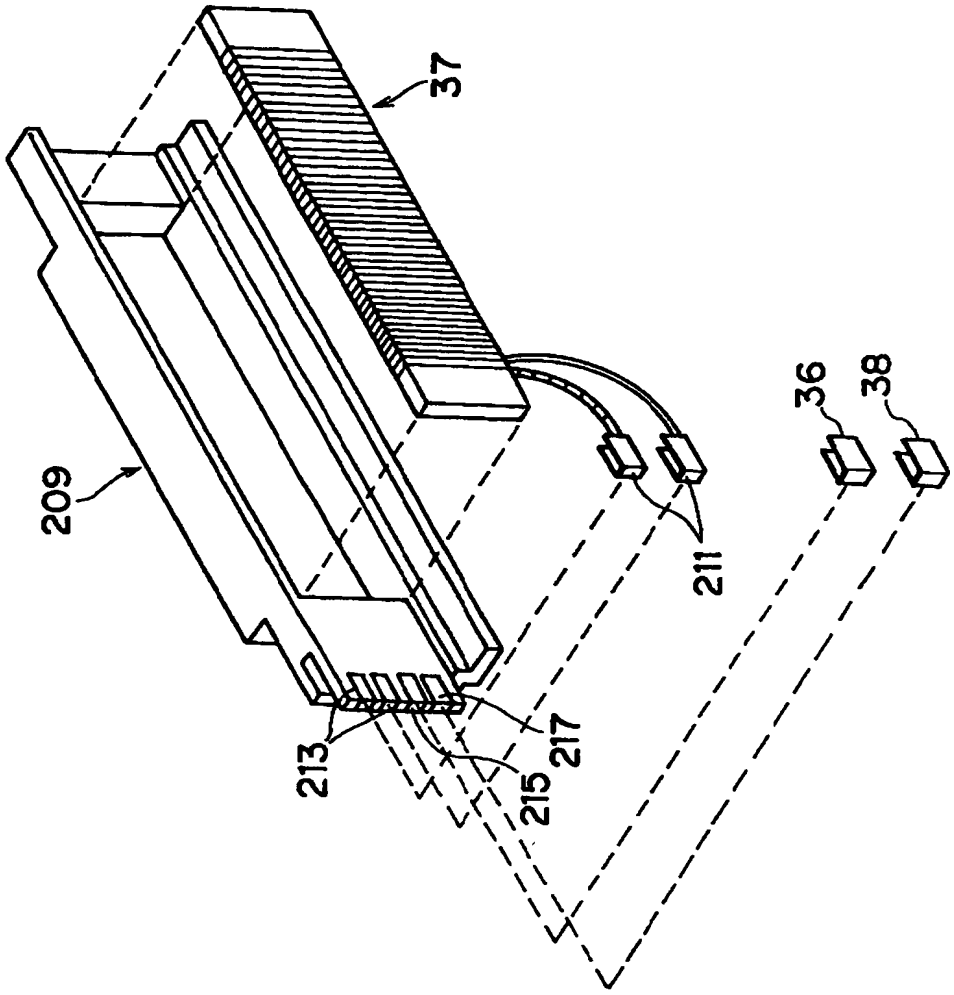
【図６】


スタート
Ｊｕｍｐｅｒ２相当の処理
89
Ｒｅｍｏｖａｌ　Ｄｅｔｅｃｔ
Ｅｎａｂｌｅ　ビット＝１？
NO
YES
アナログスイッチ遮断
95
97
ＣＭＯＳエラー？
YES
NO
1
2

【図７】



【図８】



【書類名】　　要約書

【要約】

【課題】　セキュリティ機能付きコンピュータのセキュリティ装置が不正に取り外された場合にコンピュータへのアクセスを禁止する。

【解決手段】　コンピュータの電源投入で、ＰＯＳＴプログラムが実行され、セキュリティ機能を有効にする設定で、ＲＦＩＤチップ３３は、Removal Detect Enableをハイレベルにしアナログスイッチ６７の制御側及びＮＡＮＤ素子６３の一方の入力側に出力する。ＲＦアンテナ３７が着脱されることにより第１短絡素子３６が離間され端子７１と端子７３が遮断し、素子６３のハイレベル信号でキーボード入力禁止のＩＮＴＲ信号が出力されコンピュータのアクセスを禁止する。電源オフでＲＦアンテナ着脱のときアナログスイッチ６７を遮断し、リチウムバッテリーから供給のＣＭＯＳメモリ５０への電力が遮断され、コンピュータへのアクセスを禁止することができる。

【選択図】　図２

認定・付加情報

特許出願の番号	平成１１年　特許願　第２０５３４６号
受付番号	５９９００６９５０７０
書類名	特許願
担当官	鈴木　夏生　　６８９０
作成日	平成１１年　９月　８日

＜認定情報・付加情報＞

【特許出願人】
- 【識別番号】 390009531
- 【住所又は居所】 アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
- 【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレイション

【代理人】
- 【識別番号】 100086243
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 坂口　博

【代理人】
- 【識別番号】 100091568
- 【住所又は居所】 神奈川県大和市下鶴間１６２３番地１４　日本アイ・ビー・エム株式会社　大和事業所内
- 【氏名又は名称】 市位　嘉宏

【復代理人】 申請人
- 【識別番号】 100079049
- 【住所又は居所】 東京都新宿区新宿４丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
- 【氏名又は名称】 中島　淳

【選任した復代理人】
- 【識別番号】 100084995
- 【住所又は居所】 東京都新宿区新宿４丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
- 【氏名又は名称】 加藤　和詳

【選任した復代理人】
- 【識別番号】 100085279

次頁有

認定・付加情報（続き）

【住所又は居所】　東京都新宿区新宿四丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
【氏名又は名称】　西元　勝一
【選任した復代理人】
【識別番号】　100099025
【住所又は居所】　東京都新宿区新宿４丁目３番１７号　ＨＫ新宿ビル７階　太陽国際特許事務所
【氏名又は名称】　福田　浩志

次頁無

出　願　人　履　歴　情　報

識別番号　　〔３９０００９５３１〕

１．変更年月日　　１９９０年１０月２４日
［変更理由］　新規登録
住　所　アメリカ合衆国１０５０４、ニューヨーク州　アーモンク　（番地なし）
氏　名　インターナショナル・ビジネス・マシーンズ・コーポレイション